



# Patch Readme - Linux

## HP Cloud Service Automation

Software version: CSA 4.50.0002 Patch

Publication Date: February 18, 2016

### Introduction

This document provides patch installation instructions for HP Cloud Service Automation Server (CSA) 04.50.0002 on Linux environments and describes the changes that were made to CSA version 4.50 in this update. The cumulative patch will update HP Cloud Service Automation Server to 04.50.0002.

This software patch applies to CSA version 04.50.0000 and is intended to improve the overall performance of CSA 4.50.

---

### Table of Contents

- Fixed issues..... 2
- Known issues..... 6
- Enhancements..... 10
- What's New..... 12
- Downloading and installing the patch..... 13
- Configuring Global Search in Cluster Environments..... 15
- Uninstalling the patch ..... 17
- Verifying the uninstallation..... 18
- CSA modified files ..... 18
- Appendix: Steps to configure HP CSA with CAC for SAN ..... 20
- Send documentation feedback ..... 32
- Legal notices..... 32

# Fixed issues

The following table describes the fixed issues available in this patch.

**Table 1. Fixed Issues**

Change Request	Description of fixed issue
QCCR1D189960	<p><b>Symptom:</b> When assigning a group to the CSA subscription, Groups like "Remote Desktop Users" where the user is not a member is shown.</p> <p><b>Resolution:</b> Only the groups defined in CSA for access will be displayed in the drop down list for Group Ownership.</p>
QCCR1D193127	<p><b>Symptom:</b> Unable to view the value shown in the drop-down lists while expanding the details in View Request Details, and Review Request Details.</p> <p><b>Resolution:</b> Corrected the behavior in the product.</p>
QCCR1D212278	<p><b>Symptom:</b> Approval pop-ups are shown each time an action is being started on a service component even when no approval is set for the specific action.</p> <p><b>Resolution:</b> Corrected the behavior in the product.</p>
QCCR1D212537	<p><b>Symptom:</b> Admin UI wrongly checks the input values for Offerings. It request for Display name + version to be unique, which is not correct.</p> <p><b>Resolution:</b> Allows creating a service offering that has the same display name and offering version as set for another service offering.</p>
QCCR1D212811	<p><b>Symptom:</b> Service Modification form should have "Show More Details" enabled (ON) by default.</p> <p><b>Resolution:</b> Show Details is enabled in Subscription Modification screen by default.</p>
QCCR1D213328	<p><b>Symptom:</b> When the subscription is in paused state and the subscription has an approval for cancellation, then the subscription is stuck in the pending state forever.</p> <p><b>Resolution:</b> Subscription will not be stuck in pending state under any conditions.</p>
QCCR1D213369	<p><b>Symptom:</b> Request Subscription API calls, which works for CSA 3.2 are not working on CSA 4.5.</p>

Change Request	Description of fixed issue
	<p><b>Resolution:</b> Upgraded the undertow jars.</p>
QCCR1D214030	<p><b>Symptom:</b> Subscription creation/edit is ignoring subscriber's input for a property that is unlocked but is under locked Option</p> <p><b>Resolution:</b> Subscriber input given to a property of a locked Option will be set.</p>
QCCR1D214086	<p><b>Symptom:</b> It was not possible to integrate to CSA using ccue-consumption REST API.</p> <p><b>Resolution:</b> Now we are providing 2(GET and POST) integration APIs in CSA to use the ccue-consumption REST API.</p>
QCCR1D214172	<p><b>Symptom:</b> Dynamic option JSP is not running in some cases - cached results are presented.</p> <p><b>Resolution:</b> Since Option value cache timeout is reduced to one second - instant cached results will be presented.</p>
QCCR1D214834	<p><b>Symptom:</b> API is not returning the correct date format in the XML. If the milliseconds portion of the timestamp is .000, then the API is strips the value and causes the OO date parser to fail.</p> <p><b>Resolution:</b> Added 10 millisecond delay when time has 000 millisecond value.</p>
QCCR1D215129	<p><b>Symptom:</b> Unable to receive emails when subscription processing is paused due to provisioning failure.</p> <p><b>Resolution:</b> Emails should be sent when subscription provisioning fails and pause on failure is enabled.</p>
QCCR1D215378	<p><b>Symptom:</b> While migrating design from CloudOS to HOS without saving the design, the correct HOS tag is not arrived.</p> <p><b>Resolution:</b> Corrected the behavior with adequate code changes.</p>
QCCR1D217040	<p><b>Symptom:</b> Option icons on service offering options are not displayed in the MPP.</p> <p><b>Resolution:</b> Option icons on service offering options are now added in the MPP page.</p>
QCCR1D217430	<p><b>Symptom:</b> Database Error Occurs when we request User Identifier Through Legacy API.</p>

Change Request	Description of fixed issue
	<p><b>Resolution:</b> The behavior has been corrected.</p>
QCCR1D217755	<p><b>Symptom:</b> DB error occurs when executing 2 API calls at the same time, as it doesn't allow two update queries on the same table at the same time.</p> <p><b>Resolution:</b> Parallel submit of request will not result in an exception and the subscriptions will be created successfully.</p>
QCCR1D218298	<p><b>Symptom:</b> The user options are arranged in a random way for some offerings.</p> <p><b>Resolution:</b> The Option property sorting is now based on the natural order defined in the Design.</p>
QCCR1D218404	<p><b>Symptom:</b> CSA Category Filter is only showing "Platform Services". "Database Services" and "Network Services" not displaying in the drop down list.</p> <p><b>Resolution:</b> CSA Category Filter Option will show the categories of all the subscriptions for a user.</p>
QCCR1D218711	<p><b>Symptom:</b> Some JSPs that are loading dynamic subscription options are shown as invalid when the default option is empty.</p> <p><b>Resolution:</b> The behavior in the dynamic subscription options has been rectified.</p>
QCCR1D219387	<p><b>Symptom:</b> If a display name of a Topology design contains multibyte characters, a name of the corresponding OO content pack is corrupted.</p> <p><b>Resolution:</b> The behavior has been rectified.</p>
<b>Issues fixed in 4.50.0001 patch</b>	
QCCR1D170695	<p><b>Symptom:</b> The internal action - 'Build Resource Provider and Pool List' fails to select a valid Resource Pool when used with multiple resource providers.</p> <p><b>Resolution:</b> The CSA 3.2 internal action 'Build Resource Provider and Pool List' should support multiple Providers and select a valid Resource Pool.</p>

Change Request	Description of fixed issue
QCCR1D190452	<p><b>Symptom:</b> Service Offering with a wide Optionsets takes long time to load in the MPP.</p> <p><b>Resolution:</b> Service offering with wide Option models will load quicker.</p>
QCCR1D194880	<p><b>Symptom:</b> In CSA 4.10, the selected background image for the "Dashboard Widgets" is ignored and the background remains white in MPP.</p> <p><b>Resolution:</b> HP has reviewed this change request. After careful consideration regrettably HP has determined the requested change will not be addressed within the product.</p>
QCCR1D194983	<p><b>Symptom:</b> f the Subscriber Option properties that are set to invisible in the Service Design they will reappear after the visibility of the overlaying option in the Service Offering changed.</p> <p><b>Resolution:</b> The visibility of the options in the portal are made consistent with their settings in the Offering UI.</p>
QCCR1D208427	<p><b>Symptom:</b> User should be able to view the properties of a canceled subscription.</p> <p><b>Resolution:</b> The backend code was modified to show the properties when the subscription is in cancelled state as well. Now on the services page the component properties will be shown even if the subscription is cancelled.</p>
QCCR1D208611	<p><b>Symptom:</b> After Old subscriptions are deleted from MPP and CSM and using db purge tool to cleanup db, still in MPP &gt; Notifications there are still plenty of logs left from before</p> <p><b>Resolution:</b> Corrected the behavior with the required code changes.</p>
QCCR1D208830	<p><b>Symptom:</b> Subscriber Option values from dynamic JSP pages are not loading when propertyName string used</p> <p><b>Resolution:</b> Code problem was fixed</p>
QCCR1D209136	<p><b>Symptom:</b> When the customer executes the following API call, they get a subscription count 1:</p> <p><a href="https://***.***.***.***:8444/csa/rest/user/mysubscription?userIdentifier=20f6509a49a978fe0149c8629a3e5163&amp;requestor=pvrbican_m&amp;returnRetired=true&amp;creationStartDate=2015-03-11T23:59:59">https://***.***.***.***:8444/csa/rest/user/mysubscription?userIdentifier=20f6509a49a978fe0149c8629a3e5163&amp;requestor=pvrbican_m&amp;returnRetired=true&amp;creationStartDate=2015-03-11T23:59:59</a></p> <p>After they add the creationEndDate parameter and execute the API call (and use the same startDateParameter) they get a subscription count 87 (also see</p>

Change Request	Description of fixed issue
	<p>attachment:</p> <p><a href="https://***.***.***.***:8444/csa/rest/user/mysubscription?userIdentifier=20f6509a49a978fe0149c8629a3e5163&amp;requestor=pvrbian_m&amp;returnRetired=true&amp;creationStartDate=2015-03-11T23:59:59&amp;creationEndDate=2015-03-17T23:59:59">https://***.***.***.***:8444/csa/rest/user/mysubscription?userIdentifier=20f6509a49a978fe0149c8629a3e5163&amp;requestor=pvrbian_m&amp;returnRetired=true&amp;creationStartDate=2015-03-11T23:59:59&amp;creationEndDate=2015-03-17T23:59:59</a></p> <p><b>Resolution:</b></p> <p>Modified the HQL query to solve the issue.</p>
QCCR1D209782	<p><b>Symptom:</b></p> <p>In CSA 3.2 The 'Cancel Subscription' button is still available to the end-user. If the user clicks 'Cancel Subscription' again (as they have been trained to do in this instance), CSA will continue with the next actions in the de-provisioning lifecycle. In CSA 4.2 this option is not available. Customer is requesting this feature back and does not see this as an enhancement, customer states that this is a defect and is affecting their future upgrade scheduled for July 10th.</p> <p><b>Resolution:</b></p> <p>Cancel Subscription button should be enabled in MPP UI if a subscription cancellation fails.</p>

## Known issues

The following table describes the remaining known issues in this patch.

**Table 2. Known Issues**

Change Request	Description of Known issue
QCCR1D220470	<p><b>SYMPTOM DESCRIPTION:</b></p> <p>The Cluster environment does not work after installing CSA 4.5 Patch 2 when CSA 4.5 is configured in a high availability mode.</p> <p><b>WORKAROUND:</b></p> <p>Manual configuration changes are necessary for making cluster environment work after installing CSA 4.5 Patch 2 as mentioned below:</p> <p>Search for the following</p> <pre>&lt;!--START HA Mode Configuration--&gt;</pre> <pre>&lt;!--      &lt;jee:jndi-lookup id="channelGroup" jndi- name="java:jboss/clustering/group/server" expected- type="org.wildfly.clustering.group.Group"/&gt; à</pre> <pre>&lt;!--END HA Mode Configuration--&gt;</pre> <p>Replace with</p> <pre>&lt;!--START HA Mode Configuration--&gt;</pre>

Change Request	Description of Known issue
	<pre> &lt;jee:jndi-lookup id="channelGroup" jndi- name="java:jboss/clustering/group/server" expected- type="org.wildfly.clustering.group.Group"/&gt;  &lt;!--END HA Mode Configuration--&gt; </pre>
<p>QCCR1D210391</p>	<p><b>SYMPTOM DESCRIPTION:</b> Elastic Search does not work after installing CSA 4.5 Patch 2 when CSA 4.5 is configured in a high availability mode.</p> <p><b>RESOLUTION DESCRIPTION:</b> Manual configuration changes are necessary for making Elastic Search work after installing CSA 4.5 Patch 1. These are described below:</p> <p><b>How to configure Global Search (Elasticsearch) in HA Cluster</b></p> <p>In CSA 4.5 Global search is disabled by default. Please refer to CSA Configuration Guide Chapter 7: The Marketplace Portal for details on enabling global search. When turning on Global Search in HA cluster, there are additional steps required.</p> <p>In 4.5 MR, strictSSL is not supported for elasticsearch in standalone or HA cluster mode.</p> <p>In 4.5 Patch 2, strictSSL is supported for both standalone and HA mode as long as certs are properly configured.</p> <p><b>Enabling global search in HA configuration for 4.5 Patch 2.</b></p> <ol style="list-style-type: none"> <li>1. Replace csa.properties csa.provider.msvc.hostname with local node FQDN</li> <li>2. Replace csa-search-service/app.json ccue-basic-server.host with local node FQDN</li> <li>3. Replace csa-search-service/app.json msvc-basic-search.searchEngineURL with local node FQDN</li> </ol> <p><i>If the cluster setup is using default CSA (self-signed) certificates complete the following 2 steps. (These 2 steps are not required if the cluster runs valid certificates signed by a common CA)</i></p> <ol style="list-style-type: none"> <li>4. Change csa-search-service/app.json msvc-basic-search.strictSSL/rejectUnauthorized: false</li> <li>5. Change elasticsearch/config/elasticsearch.yml searchguard.ssl.transport.http.enforce_clientauth: false</li> </ol> <p><i>Verify the following HA configurations in csa-search-service/app.json are maintained after the installation of the patch.</i></p> <ol style="list-style-type: none"> <li>6. idmURL should point to the load balancer <i>example:</i> "idmURL": "<a href="https://http-loadbalancer.csapcoe.hp.com:8443/idm-service">https://http-loadbalancer.csapcoe.hp.com:8443/idm-service</a>" <i>Port 8443 is the Load balancer port which was configured manually during CSA 4.5 MR installation.</i></li> <li>7. cert should point to the load balancer cert <i>example:</i> "ca": "<i>C:/Program Files/Hewlett-Packard/CSA/jboss-as/standalone/configuration/apache_csa.crt</i>" <i>Name of crt cannot remain as jboss.crt which is set as default.</i></li> </ol> <p><i>For more information on setting up certificates please refer to the following documents:</i></p>

Change Request	Description of Known issue
	<p style="text-align: center;"><i>FIPS 140-2 Compliance Configuration Guild</i></p> <p style="text-align: center;"><i>CSA 4.5 Cluster Configuration for High Availability Using an Apache Web Server</i></p>
QCCR1D210453	<p><b>SYMPTOM DESCRIPTION:</b></p> <p>Option Model property editor for Topology Designs would allow users to select token values for List type properties based on dynamic options JSP files. After selecting a token value, users are able to modify the token value in the value input field.</p> <p>Modifying token values in Option Model property editor causes problems when retrieving property values from Marketplace Portal during service creation.</p> <p><b>WORKAROUND:</b></p> <p>Do not edit token value after selecting a token from available list of token for List type properties in Option Model property editor.</p>
QCCR1D210590	<p><b>SYMPTOM DESCRIPTION:</b></p> <p>Various issues are seen when using Google Chrome version 44 to browse Service Management Console and Marketplace Portal when CSA is setup with self signed certificates.</p> <ol style="list-style-type: none"> <li>1. After browsing for about ten minutes, the browser is automatically redirected to a security page with title "Your connection is not private" where users usually trust self signed certificates.</li> <li>2. After browsing for some time, blank pages are displayed when navigating from one page to another.</li> <li>3. An error message such as "An error has occurred. Cannot connect to the server. Check your network connection please" is displayed after browsing for some time.</li> </ol> <p><b>WORKAROUND:</b></p> <p>Versions of Google Chrome prior to version 44 do not have these problems. Other browsers such as Internet Explorer and Mozilla Firefox also do not have these problems.</p> <p>On Google Chrome version 44, trusting the self signed certificate by adding the certificate to 'Trusted Root Certificate Authorities' also seems to be solving this issue.</p>
QCCR1D211195	<p><b>SYMPTOM DESCRIPTION in customer terms:</b></p> <p>Service topology view of a service subscription from Marketplace Portal does not show the state of a service component when users hover upon the icon which displays state of the service component. This problem is only limited to Internet Explorer 11.</p> <p><b>WORKAROUND:</b></p> <p>This problem is only limited to Internet Explorer 11. State of a service component is visible when using Google Chrome or Mozilla Firefox browsers to view the service topology view of a service subscription by hovering on a service component state icon.</p>
QCCR1D211202	<p><b>SYMPTOM DESCRIPTION in customer terms:</b></p> <p>CSA ships a few out of the box OpenStack Service Designs. These Service Designs utilize dynamic option JSP files in Option Model. Opening a Service Offering based on these designs for the purpose of ordering a service from Marketplace Portal leads to the webpage being frozen. When this happens users are unable to order a service from this Service Offering.</p>



Change Request	Description of Known issue
	<p><b>WORKAROUND:</b></p> <p>Logging out of Marketplace Portal and logging back-in fixes this issue.</p>
QCCR1D207419	<p><b>SYMPTOM DESCRIPTION:</b></p> <p>When IDM created the SSO cookie no audit logging was done.</p> <p><b>WORKAROUND:</b></p> <p>In order to enable user login auditing for an SSO configured CSA 4.50.0002, the following property needs to be added to any un-commented SSOFilter bean in the /idm-service.war/WEB-INF/spring/applicationContext-security.xml file.</p> <pre data-bbox="418 657 1089 684">&lt;property name="auditAppender" ref="auditAppender"/&gt;</pre> <p>For example:</p> <p>Before change:</p> <pre data-bbox="513 783 1503 1073">&lt;bean id="ssoFilter" class="com.hp.ccue.identity.filter.sso.SSOFilter"&gt;     &lt;property name="generateTokenUtil" ref="generateTokenUtil" /&gt;     &lt;property name="tokenFactory" ref="tokenFactory" /&gt;     &lt;property name="loginRedirectionHandler" ref="loginRedirectionHandler" /&gt; &lt;/bean&gt;</pre> <p>After change:</p> <pre data-bbox="513 1136 1503 1499">&lt;bean id="ssoFilter" class="com.hp.ccue.identity.filter.sso.SSOFilter"&gt;     &lt;property name="generateTokenUtil" ref="generateTokenUtil" /&gt;     &lt;property name="tokenFactory" ref="tokenFactory" /&gt;     &lt;property name="loginRedirectionHandler" ref="loginRedirectionHandler" /&gt;     &lt;property name="auditAppender" ref="auditAppender"/&gt; &lt;/bean&gt;</pre>

# Enhancements

The following table describes the fixed issues available in this patch.

**Table 3. Fixed Issues**

Change Request	Description of fixed issue
QCCR1D201403	<p><b>Symptom:</b> CSA currently uses the out-of-the-box Spring provided CAC filter that provides a regex to parse only the Subject field.</p> <p><b>Resolution:</b> Fixed the issue to support subjectDN and subjectAltName attributes ( rfc822Name and OtherName for UPN) of X.509 certificate.</p>
QCCR1D208162	<p><b>Symptom:</b> Service Request does not track the completeness of the Subscription.</p> <p><b>Resolution:</b> The state/status and completedOn timestamp of the service request was updated appropriately for various actions like order.modify,cancel action.</p>
QCCR1D209226	<p><b>Symptom:</b> In the email confirming the rejection of a request towards an end user, the reason is not specified even though this is given in the portal.</p> <p><b>Resolution:</b> An enhancement has been made to the product in 4.2 patch release to include the approver's comment for rejection.</p>
<b>Issues fixed in 4.50.0001 patch</b>	
QCCR1D188066	<p><b>Symptom:</b> Inability to read the catalog ID in the dynamic query JSPs, by adding the SVC_CATALOG_ID token to the list of available tokens in the dynamic query http body.</p> <p><b>Resolution:</b> The catalog ID - *[PORTAL: CATALOG_ID] *should be available now for usage.</p>
QCCR1D209730	<p><b>Symptom:</b> The logged in user id was not right when the group subscription was set up. It was always the user id of the one who created it.</p> <p><b>Resolution:</b> More tokens have been added and also the user id shown will be the logged in user id.</p>
QCCR1D210180	<p><b>Symptom:</b> Consumer admin is able to create service offerings from MPP and potentially set zero pricing</p>

Change Request	Description of fixed issue
	<p><b>Resolution:</b></p> <p>The ability to turn off 'Offering Management' widget from Marketplace Portal for Consumer Organization Administrators has been introduced. This will solve the problem where a Consumer Organization Administrator could create Service Offerings with zero pricing. When 'Offering Management' widget is turned off from Marketplace Portal, Consumer Organization Administrators will only be able to add service offerings created in Service Management Console through Marketplace Portal's 'Catalog Management' widget.</p> <p>Follow below steps to turn off 'Offering Management' widget from Marketplace Portal for Consumer Organization Administrators:</p> <p>To remove the Offering Management tile for the Tenant Admin:</p> <ol style="list-style-type: none"> <li>1. Open {CSA_Installation_Folder} /portal/conf/dashboard.json in a text editor.</li> <li>2. Find "MANAGE_OFFERINGS".</li> <li>3. Remove the object that has the label "common.items.MANAGE_OFFERINGS". The whole object looks like: <pre> {   "label": "common.items.MANAGE_OFFERINGS",   "icon": {     "className": "icon-services"   },   "className": "orange",   "link": {     "url" : "consumption/offerings/ ",     "target": "_blank"} } </pre> </li> <li>4. Open {CSA_Installation_Folder}/portal/conf/mpp.json in a text editor.</li> <li>5. Find "enableOfferingAdministration".</li> <li>6. Set the consumption.enableOfferingAdministration property to false.</li> <li>7. Restart HP Marketplace Portal service</li> </ol>
QCCR1D210054	<p><b>Symptom:</b></p> <p>Need to ability to disable security warning banner</p> <p><b>Resolution:</b></p> <ol style="list-style-type: none"> <li>1.To change security warnings in the MPP: <ol style="list-style-type: none"> <li>a.Open the MPP dashboard file in a text editor: CSA_HOME/portal/conf/dashboard.json</li> <li>b.Find the "header.securityWarning.enable" parameter and set to desired value (true or false).</li> </ol> </li> <li>2.To change security warnings for the MPP Tenant Admin: <ol style="list-style-type: none"> <li>a.Open the MPP config file in a text editor: CSA_HOME/portal/node_modules/mpp-consumption/dist/offerings/config.json</li> <li>b.Find the "enableSecurityWarning" parameter and set to desired value (true or false).</li> </ol> </li> <li>3.Documentation for changing security warnings in the SCM:</li> </ol>

Change Request	Description of fixed issue
	<p>a. Open the Service Management Console config file in a text editor: CSA_HOME/jboss-as/standalone/deployments/csa.war/offerings/config.json</p> <p>b. Find the "enableSecurityWarning" parameter value and set to desired value (true or false).</p>

---

## What's New

In CSA Cluster Configuration using Apache Server, the documentation suggests to generate a certificate with sha1. In this patch, we will have to replace sha1 with sha256, as described below.

To generate the certificate and private key, replace the following command:

```

` openssl req -new -x509 -days 365 -sha1 -newkey rsa:2048 -nodes
-keyout /etc/httpd/conf/apache_csa.key
-out /etc/httpd/conf/apache_csa.crt
-config /etc/httpd/conf/openssl.cnf
-subj /O=HP/OU=HP/CN=[APACHE_LOAD_BALANCER_HOSTNAME] `

```

With this:

```

` openssl req -new -x509 -days 365 -sha256 -newkey rsa:2048 -nodes
-keyout /etc/httpd/conf/apache_csa.key
-out /etc/httpd/conf/apache_csa.crt
-config /etc/httpd/conf/openssl.cnf
-subj /O=HP/OU=HP/CN=[APACHE_LOAD_BALANCER_HOSTNAME] `

```

### CAC configuration for subject/SAN based authentication

CAC is enabled in HP CSA for SAN based authentication. Refer [Appendix](#) for Steps to configure HP CSA with CAC.

---

# Downloading and installing the patch

## Pre-installation requirements

Before installing the patch:

1. Make sure that your system meets the following minimum requirements:
  - a. Minimum hardware:
    - i. CPU: 4 CPU, 3.0 GHz
    - ii. RAM: 8 GB
    - iii. Hard Drive: 20 GB
  - b. Operating system:

For supported operating systems details, see HP CSA 4.50 Support Matrix available at: <https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01691511>
  - c. Software:

Version 4.50.0000 of HP Cloud Service Automation
2. Back up the CSA environment.
3. Make sure that new subscriptions are not being created and that existing subscriptions are not being modified when this patch installer is being applied.

**Important:** Failing to do this can leave CSA in an unstable state and the patch application can fail.

- a. Sign out of all open instances of the HP CSA Provider Console and HP Marketplace Portal.
- b. Stop the following CSA Services:
  - i. HP Cloud Service Automation,
  - ii. HP Marketplace Portal,
  - iii. HP Search and
  - iv. Elasticsearch 1.5.2 services.

**Important:** For clustered CSA servers, stop the services on all nodes.

## Installing the patch on standalone CSA servers

To install the patch in a standalone configuration:

1. Complete prerequisite steps described under [Pre-installation requirements](#).
2. Download the CSA patch file.
3. Extract the `HP_CSA_Patch_04.50.0002.bin` file from the patch tar file.
4. Verify that `HP_CSA_Patch_04.50.0002.bin` is owned by the 'csauser' user and that csauser has full permissions to the file. If necessary, do the following:
  - a. Log in as the root user and enter the following commands:

```
chown csauser:csagrps HP_CSA_Patch_04.50.0002.bin
chmod u+rwxs HP_CSA_Patch_04.50.0002.bin
```
  - b. Log out as the root user.
5. Log in as csauser and run `HP_CSA_Patch_04.50.0002.bin` to open the console mode of the HP Cloud Service Automation Patch Installer.

6. Enter `./HP_CSA_Patch_04.50.0002.bin` to initiate the patch installer interview.
7. Acknowledge information screens and warnings:
  - a. Read the introduction and click **Enter**.
  - b. Read warnings to stop services and comply with instructions before proceeding to the next step. To acknowledge you have completed the required pre-requisites, click **Enter**.
8. Select **Standalone** as the HP CSA environment option, and click **Enter**.
9. Select the option that describes your set-up and click **Next**:
  - a. Select **CSA and MPP are installed** if both the components are installed.
  - b. Select **Only MPP is installed** if only MPP is installed.

**Note:** If you selected **Only MPP**, perform the same steps to install the patch, but ignore the configurations that are specific to JBoss and `csa.war`.
10. Review the pre-installation summary and click **Enter** to run the complete patch installation.
11. After the installation completes, click **Enter** to exit.
12. Verify the installation and restart services as instructed below under [Verifying the installation](#).

## Installing the patch on clustered CSA servers

To install the patch in a clustered environment, perform these steps on all nodes of the CSA cluster:

1. Complete prerequisite steps described under [Pre-installation requirements](#).
2. Download the patch file.
3. Extract the `HP_CSA_Patch_04.50.0002.bin` file from the patch tar file.
4. Verify that `HP_CSA_Patch_04.50.0002.bin` is owned by the 'csauser' user and that csauser has full permissions to the file. If necessary, do the following:
  - a. Log in as the root user and enter the following commands:
 

```
chown csauser:csagrp HP_CSA_Patch_04.50.0002.bin chmod u+rwx
HP_CSA_Patch_04.50.0002.bin
```
  - b. Log out as the root user.
5. Log in as csauser and run `HP_CSA_Patch_04.50.0002.bin` to open the console mode of the HP Cloud Service Automation Patch Installer.
6. Enter `./HP_CSA_Patch_04.50.0002.bin` to initiate the patch installer interview.
7. Acknowledge information screens and warnings:
  - a. Read the introduction and click **Enter**.
  - b. Read warnings to stop services and comply with instructions before proceeding to the next step. To acknowledge you have completed the required pre-requisites, click **Enter**.
8. Select **Cluster** as the HP CSA environment option, and click **Enter**.
9. Select the option that describes your set-up and click **Next**:
  - a. Select **CSA and MPP are installed** if both the components are installed.
  - b. Select **Only MPP is installed** if only MPP is installed.

**Note:** If you selected **Only MPP**, perform the same steps to install the patch, but ignore the configurations that are specific to JBoss and `csa.war`.
10. Review the pre-installation summary and click **Enter** to run the complete patch installation.
11. After the installation completes, click **Enter** to exit.
12. Verify the installation and restart services as instructed below under [Verifying the installation](#).

## Verifying the installation

The verification steps apply to both standalone and clustered environments. For clustered environments, complete these steps on each node after completing the installation on each node.

1. Check the logs for any errors under  
`$CSA_HOME/_CSA_4_50_2_installation/Logs`  
The log files include:
  - `csa_install.log`
  - `csa_InstallPatch.log`
  - `upgradeidm.log`
  - `upgrade_search_service.log`
2. Ensure that the browser cache is cleared.
3. Start the following services if they are not already running:
  - a. HP Cloud Service Automation
  - b. HP Marketplace Portal
  - c. HP Search
  - d. Elasticsearch

**Note:** For Linux, after the patch installation is complete, start the services manually.

**Important:** In a clustered environment, make sure services are started on all nodes.

4. Launch the Cloud Service Management Console, log in, and then check for the updated version.

**Note:** If there are errors in the log files, create a backup of the log files, restore the backup of the `CSA_HOME` directory, and contact HP Support.

**Important:** If the patch is installed in a cluster environment, Elasticsearch will be non-functional if it was enabled prior to the patch installation. In order to make global search functional, follow the steps defined in the "Configuring Elasticsearch in Cluster Environments."

---

## Configuring Global Search in Cluster Environments

Manual configuration changes are necessary for making Global Search work after installing CSA 4.50 Patch 1, as described below.

StrictSSL support for Elasticsearch:

- In 4.50 MR, strictSSL is not supported for Elasticsearch in standalone or HA cluster mode.
- In 4.50 Patch 2, strictSSL is supported for Elasticsearch for both standalone and HA mode as long as the certificates are properly configured.

### How to configure Elasticsearch in a High Availability (HA) cluster

In CSA 4.5 Global Search is disabled by default. For instructions on enabling Global Search, see Chapter 7: The Marketplace Portal in the *CSA 4.50 Configuration Guide*.

After completing the steps described in the aforementioned configuration guide, the following additional steps are required when turning on Global Search in an HA cluster environment.

1. Go to `csa.properties`, locate `csa.provider.msvc.hostname` and replace with local node FQDN.
1. Go to `csa-search-service/app.json`, locate `ccue-basic-server.host` and replace with local node FQDN.
2. Go to `csa-search-service/app.json`, locate `msvc-basic-search.searchEngineURL` and replace with the local node FQDN.
3. Complete the certificate set-up appropriate steps for your environment:
  - a. If the cluster setup is using the default CSA (self-signed) certificates change the following settings to "false."

**(Note: These 2 settings do not need to be modified if the cluster runs valid certificates signed by a common CA.)**

```
csa-search-service/app.json msvc-basic-search.strictSSL/rejectUnauthorized:
false
elasticsearch/config/elasticsearch.yml
searchguard.ssl.transport.http.enforce_clientauth: false
```

- b. Verify the following HA configurations in `csa-search-service/app.json` are maintained after the installation of the patch:
  - i. `idmURL` should point to the load balancer  
 For example:  
`"idmURL": "https://http-loadbalancer.csapcoe.hp.com:8443/idm-service"`  
 where Port 8443 is the load balancer port that was configured manually during CSA 4.5 MR installation.
  - ii. `cert` should point to the load balancer cert  
 For example:  
`"ca": "C:/Program Files/Hewlett-Packard/CSA/jboss-as/standalone/configuration/apache_csa.crt"`  
 The above example has apache as load balancer cert  
`.crt` should be replaced with the selected load balancer certificate.

For more information on setting up certificates please refer to the following CSA 4.50 documents:

Document	Link to CSA 4.50 document on the SSO
FIPS 140-2 Compliance Statement	<a href="https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01691504">https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01691504</a>
FIPS Compliance Configuration Guide	<a href="https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01702243">https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01702243</a>
Configuring an HP CSA Linux Cluster for High Availability Using an Apache Web Server	<a href="https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01737522">https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01737522</a>
Configuring an HP CSA Windows Cluster for High Availability Using an Apache Web Server	<a href="https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01737523">https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM01737523</a>

**Note:** Please see the [CSA 4.x Documentation Library](#) on the HP Software Support Online (SSO) portal for links to all product documentation. (HP Passport is required.)



---

# Uninstalling the patch

## Preparing for uninstallation

1. Backup the CSA environment.
2. Make sure that new subscriptions are not being created and that existing subscriptions are not being modified when this patch installer is being applied.

**Important:** Failing to do this can leave CSA in an unstable state and the patch application can fail.

- a. Sign out of all open instances of the HP CSA Provider Console and HP Marketplace Portal.
- b. Stop the following CSA Services:
  - i. HP Cloud Service Automation,
  - ii. HP Marketplace Portal,
  - iii. HP Search and
  - iv. Elasticsearch 1.5.2 services.

**Important:** For clustered CSA servers, stop the services on all nodes.

## Uninstalling the patch on standalone CSA servers

To uninstall the patch in a standalone configuration:

1. Complete prerequisite steps described under [Preparing for uninstallation](#).
2. Navigate to the `$CSA_HOME/_CSA_4_50_2_installation/Uninstaller` folder.
3. Run `./Uninstall HP Cloud Service Automation Patch` to start the console mode of the patch uninstaller.
4. Read the introduction and click **Enter**.
5. Read warnings to stop services and comply with instructions before proceeding to the next step. Verify you have completed the required pre-requisites.
6. Click **Enter** to run the patch uninstaller.
7. After the uninstallation completes, click **Enter** to exit.
8. Verify the uninstallation and restart services as instructed under [Verifying the uninstallation](#).

## Uninstalling the patch on clustered CSA servers

To uninstall the patch in a clustered environment, perform these steps on all nodes of the CSA cluster:

1. Complete prerequisite steps described under [Preparing for uninstallation](#).
2. Navigate to the `$CSA_HOME/_CSA_4_50_2_installation/Uninstaller` folder.
3. Run `./Uninstall HP Cloud Service Automation Patch` to start the console mode of the patch uninstaller.
4. Read the introduction and click **Enter**.
5. Read warnings to stop services and comply with instructions before proceeding to the next step. To acknowledge you have completed the required pre-requisites.
6. Click **Enter** to run the patch uninstaller.
7. After the uninstallation completes, click **Enter** to exit.

8. Verify the uninstallation and restart services as instructed under [Verifying the uninstallation](#).

---

## Verifying the uninstallation

The verification steps apply to both standalone and clustered environments. For clustered environments, complete these steps on each node after completing the uninstallation on each node.

1. Verify the logs for any errors under  
`$CSA_HOME$/_CSA_4_50_2_installation/Logs`  
The uninstall log files include:
  - `csa_uninstall.log`
  - `csa_UninstallPatch.log`
2. Ensure that the browser cache is cleared.
3. Start the following services if they are not already running:
  - a. HP Cloud Service Automation
  - b. HP Marketplace Portal
  - c. HP Search
  - d. Elasticsearch 1.5.2

For Linux, after the patch installation is complete, start the services manually.

**Important:** In a clustered environment, make sure services are started on all nodes.

---

## CSA modified files

```
<CSA_HOME>/jboss-as/standalone/deployments/csa.war/*
<CSA_HOME>/jboss-as/standalone/deployments/idm-service.war/*
<CSA_HOME>/portal/*

<CSA_HOME>/jboss-as/standalone/configuration/standalone.xml
<CSA_HOME>/jboss-as/standalone/configuration/standalone-full-ha.xml

<CSA_HOME>/jboss-as/modules/system/layers/base/io/undertow/core/main/module.xml
<CSA_HOME>/jboss-as/modules/system/layers/base/io/undertow/core/main/undertow-
core-1.1.0.Final.jar
<CSA_HOME>/jboss-as/modules/system/layers/base/io/undertow/servlet/main/module.xml
<CSA_HOME>/jboss-as/modules/system/layers/base/io/undertow/servlet/main/undertow-
servlet-1.1.0.Final.jar
<CSA_HOME>/jboss-
as/modules/system/layers/base/io/undertow/websocket/main/module.xml
<CSA_HOME>/jboss-
as/modules/system/layers/base/io/undertow/websocket/main/undertow-websockets-jsr-
1.1.0.Final.jar
```

```
<CSA_HOME>/jboss-  
as/modules/system/layers/base/org/apache/commons/collections/main/commons-  
collections-3.2.1.jar  
<CSA_HOME>/jboss-  
as/modules/system/layers/base/org/apache/commons/collections/main/module.xml
```

```
<CSA_HOME>/elasticsearch-1.5.2/config/*
```

```
<CSA_HOME>/CSAKit-4.5/OO Flow Content/10X/EXISTING-INFRASTRUCTURE-WINDOWS-cp-  
1.50.0000.jar  
<CSA_HOME>/CSAKit-4.5/OO Flow Content/10X/oo10-csa-cp-4.50.0000.jar  
<CSA_HOME>/CSAKit-4.5/OO Flow Content/10X/oo10-csa-integrations-cp-4.50.0000.jar  
<CSA_HOME>/CSAKit-4.5/OO Flow Content/10X/oo10.50-csa-integrations-cp-  
4.50.0001.jar  
<CSA_HOME>/CSAKit-4.5/OO Flow Content/9X/CSA-4_10-ContentInstaller.jar
```

```
<CSA_HOME>/Tools/ComponentTool/*  
<CSA_HOME>/Tools/ContentArchiveTool/CODAR_BP_EXISTING_WINDOWS_SERVER_COMPONENT_v1.  
50.00.zip  
<CSA_HOME>/Tools/ContentArchiveTool/content-archive-tool.jar  
<CSA_HOME>/Tools/DBPurgeTool/db-purge-tool.jar  
<CSA_HOME>/Tools/PasswordUtil/passwordUtil-standalone.jar  
<CSA_HOME>/Tools/ProcessDefinitionTool/process-defn-tool.jar  
<CSA_HOME>/Tools/ProviderTool/provider-tool.jar  
<CSA_HOME>/Tools/SchemaInstallationTool/*  
<CSA_HOME>/Tools/SupportTool/support-tool.jar
```

---

## Appendix: Steps to configure HP CSA with CAC for SAN

CSA supports 'subjectDN' and 'subjectAlternativeName' (SAN) X.509 attributes. An IT admin should be able to configure CSA to enable support for both attributes (subject' and SAN) in the same CSA instance. The IT admin can also configure CSA to support only one of the attributes if desired.

- If 'subject' attribute is enabled, then the IT admin can customize the default regex used to extract the username information from it.
- If 'SAN' is enabled, then the IT admin needs to specify one 'Name' that contains the username information. CSA will support 2 SAN Names. They are 'rfc822Name' and 'otherName'. The 'otherName' will be further restricted to only support the OID for UPN (1.3.6.1.4.1.311.20.2.3). For 'SAN' there won't be a regex to customize the extraction of the user information. Please refer to the section "LDAP server configuration for CAC authentication based on UPN" to configure the LDAP server for CAC authentication based on UserPrincipalName (UPN).
- Consider the scenario where the IT admin enables both SAN and 'subject' attributes in CSA. In this scenario, assume that CSA receives a user certificate that has the SAN attribute as well as the subject attribute populated. In this scenario CSA will try to parse the username from the 'SAN' attribute based on the 'Name' configured in CSA. If authentication fails on the username value (e.g. CSA cannot find the user in LDAP), CSA will report an Authentication failure. In the scenario where SAN attribute is not present in the user certificate then CSA will try to authenticate the user based on the 'Subject' attribute.

### Steps to configure HP CSA with CAC for SAN (SubjectAlternativeName)/SubjectDN based authentication

Please ensure that CAC is enabled in CSA as per the steps provided in the CSA Configuration Guide before making the changes provided in the below mentioned sections.

## Stop HP CSA

To stop HP CSA:

1. On the server that hosts HP Cloud Service Automation, navigate to **Start >Administrative Tools > Services**.
2. Click HP Cloud Service Automation service and select **Stop**.
3. Click HP Marketplace Portal service and select **Stop**.
4. If you installed an embedded HP Operations Orchestration instance, Click HP Operations Orchestration Central service and select **Stop**.
5. If you enabled global search, do the following:
  - a. Click the Elasticsearch 1.5.2 service and select **Stop**. You do not need to stop this service if global search is disabled (by default, global search is disabled).
  - b. Click HP Search Service and select **Stop**. You do not need to stop this service if global search is disabled (by default, global search is disabled).

# Configure the Cloud Service Management Console

1. Change the following properties in `csa.properties` file. Take a backup of the file before adding the properties.

PropertyName	Comments
<code>csa.cac.x509Attribute</code>	<p>This is the name of the X.509 certificate attribute from which the username will be extracted.</p> <p>Set this property to <code>subjectDN</code> or <code>san</code> or <code>subjectDN,san</code>. If this property is set to contain both attributes i.e. <code>subjectDN,san</code> or <code>san,subjectDN</code>, then username will be extracted from <code>subjectDN</code> attribute only if SAN attribute is not present in the certificate. If this property is not set, then the default value for the property is <code>subjectDN</code>.</p>
<code>csa.cac.regex</code>	<p>The regular expression used to extract a username from the <code>subjectDN</code> X.509 attribute. If this property is not set, then the default regex is <code>CN=(.*)</code>. This property need not be set if the property <code>csa.cac.x509Attribute</code> is set to <code>san</code>.</p>
<code>csa.cac.san.type</code>	<p>The type of the subject alternative name. The allowed types are <code>othername</code> and <code>rfc822name</code>. If this property is not set, then the default value for the property is <code>otherName</code>. This property need not be set if <code>csa.cac.x509Attribute</code> is set to <code>subjectDN</code>.</p>

Sample –

#Name of the X.509 certificate attribute from which the username will be extracted.

#Set this property to `subjectDN` or `san` or `subjectDN,san`.

#If this property is set to contain both attributes i.e. `subjectDN,san` or `san,subjectDN`, then username will be extracted from `subjectDN` attribute only if SAN attribute is not present in the certificate.

#If this property is not set, then the default value for the property is `subjectDN`.

**`csa.cac.x509Attribute=san`**

#The regular expression used to extract a username from the `subjectDN` X.509 attribute. If this property is not set, then the default regex is `CN=(.*)`.

**`#csa.cac.regex=CN=(.*)`**,

#The type of the subject alternative name. The allowed types are `othername` and `rfc822name`. If this property is not set, then the default value for the property is `otherName`.

**`csa.cac.san.type=otherName`**

2. Navigate to the `$CSA_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/directory`.

3. Take a backup copy of applicationContext-security.xml file.
4. Update the Spring Security configuration. Open the \$CSA\_HOME/jboss-as/standalone/deployments/csa.war/WEB-INF/applicationContext-security.xml file in a text editor and make the following changes:

- a. Locate the line "`<!-- Pre-authentication for CAC -->`" and uncomment the line below the same so that it appears as follows.

```
<!-- Pre-authentication for CAC -->
<security:authentication-provider ref="customX509AttrPreAuthAuthProvider"/>
```

- b. Locate both occurrences of the "x509 and custom filter config for CAC" comment and remove both occurrences of the following line. Please ignore this step if the entries are not found.

```
<x509 subject-principal-regex="CN=(.*?), " user-serviceref="
cacUserDetailsService" />
```

- c. Locate and uncomment both occurrences of the following line. Please ignore if it's already uncommented.

```
<custom-filter position="LAST" ref="cacFilter" />
```

- d. Locate both occurrences of the line "`<custom-filter position="X509_FILTER" ref="cacX509AuthenticationFilter" />`" and uncomment the same so that it appears as follows.

```
<custom-filter position="X509_FILTER" ref="cacX509AuthenticationFilter" />
```

- e. Locate the following lines.

```
<beans:bean id="cacUserDetailsService"
class="com.hp.csa.authn.impl.CACUserDetailsServiceImpl">
    <beans:property name="restRole" value="ROLE_REST" />
</beans:bean>
<beans:bean id="cacFilter" class="com.hp.csa.security.CACFilter" />
```

Uncomment the content below the above lines so that it appears as follows.

```
<!-- Bean definitions for CAC -->
<beans:bean id="cacUserDetailsService"
class="com.hp.csa.authn.impl.CACUserDetailsServiceImpl">
    <beans:property name="restRole" value="ROLE_REST" />
</beans:bean>
<beans:bean id="cacX509AuthenticationFilter"
class="org.springframework.security.web.authentication.preauth.x509.X509Authenticati
tionFilter">
    <beans:property name="authenticationManager"
ref="authenticationManager" />
    <beans:property name="principalExtractor"
ref="customX509Extractor" />
</beans:bean>

<beans:bean id="customX509AttrPreAuthAuthProvider"
class="org.springframework.security.web.authentication.preauth.PreAuthenticatedAut
henticationProvider">
    <beans:property name="preAuthenticatedUserDetailsService"
ref="customAuthenticationUserDetailsService" />
</beans:bean>
```

```
<beans:bean id="customAuthenticationUserDetailsService"
class="org.springframework.security.core.userdetails.UserDetailsServiceWrapper">
    <beans:property name="userDetailsService" ref="cacUserDetailsService"
/>
</beans:bean>

<beans:bean id="customX509Extractor"
class="com.hp.csa.security.CustomX509PrincipalExtractor">
    <beans:property name="x509Attribute"
value="\${csa.cac.x509Attribute:subjectDN}"/>
    <beans:property name="regex" value="\${csa.cac.regex:CN=(.*?),}"/>
    <beans:property name="sanType"
value="\${csa.cac.san.type:otherName}"/>
</beans:bean>
```

**5. Save the file and exit.**

# Configure the Marketplace Portal

Complete the following steps to integrate the Marketplace Portal with CAC:

1. Change the following properties in `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/spring/applicationContext.properties` file. Take a backup of the file before adding the properties.

PropertyName	Comments
<code>idm.cac.x509Attribute</code>	<p>This is the name of the X.509 certificate attribute from which the username will be extracted.</p> <p>Set this property to <code>subjectDN/san/subjectDN,san</code>. If this property is set to contain both attributes i.e. <code>subjectDN,san</code> or <code>san,subjectDN</code>, then username will be extracted from <code>subjectDN</code> attribute only if <code>SAN</code> attribute is not present in the certificate. If this property is not set, then the default value for the property is <code>subjectDN</code>.</p>
<code>idm.cac.regex</code>	<p>The regular expression used to extract a username from the <code>subjectDN X.509</code> attribute. If this property is not set, then the default regex is <code>CN=(.*?)</code>. This property need not be set if the property <code>csa.cac.x509Attribute</code> is set to <code>san</code>.</p>
<code>idm.cac.san.type</code>	<p>The type of the subject alternative name. The allowed types are <code>othername</code> and <code>rfc822name</code>. If this property is not set, then the default value for the property is <code>otherName</code>. This property need not be set if <code>csa.cac.x509Attribute</code> is set to <code>subjectDN</code>.</p>

Sample –

```
# Name of the X.509 certificate field from which the user name will be extracted.
# Possible values are:
# - subjectDN
# - san
# - subjectDN,san (or san,subjectDN)
# When the third comma separated value is used,
# If this property is not set, then the default value is subjectDN.
idm.cac.x509Attribute=san

# The regular expression used to extract a user name from the field defined by the
idm.cac.x509Attribute property.
# If this property is not set, then the default value is: CN=(.*?),
#idm.cac.regex=CN=(.*?),
```



```

# Type of the subject alternative name.
# Possible values are:
# - OtherName
# - RFC822Name
# If this property is not set, then the default value is OtherName
# Any other value is treated as an error.
idm.cac.san.type=OtherName

```

2. If HP SSO is configured for Marketplace Portal, then please refer to section “Configure Marketplace Portal for CAC authentication based on SAN when SSO is enabled”.
3. Navigate to the \$CSA\_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/spring directory.
4. Take a backup copy of “applicationContext-security.xml” file.
5. Edit the \$CSA\_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/spring/applicationContext-security.xml file:

- a. Locate the “<!-- START Certificate Authentication Configuration -->” section. If you are not using HP SSO, locate and comment the “<!-- START without HP SSO support -->” section so that it appears as follows. Please ignore if this is already commented.

```

<!-- START without HP SSO support -->
  <!--
    <security:http pattern="/idm/v0/login" use-expressions="true" auto-
    config="false">
      <security:http-basic />
      <security:custom-filter ref="requestTokenCompositeFilter"
    position="FIRST"/>
      <security:x509 subject-principal-regex="CN=(.*?)," user-service-
    ref="cacUserDetailsService" />
      <security:custom-filter position="LAST" ref="cacFilter" />
    </security:http>

    <bean id="cacFilter"
    class="com.hp.ccue.identity.filter.certificate.CertificateFilter">
      <property name="generateTokenUtil" ref="generateTokenUtil" />
      <property name="tokenFactory" ref="tokenFactory"/>
      <property name="loginRedirectionHandler" ref="loginRedirectionHandler"/>
      <property name="authenticationProvider" ref="cacLdapAuthProvider"/>
    </bean>-->

```

- b. Locate the line “<!-- START Certificate Authentication Configuration with subjectAlternativeName authentication --><!-- (without HP SSO support) -->” and uncomment the contents below the same so that it appears as follows.

```

<!-- START Certificate Authentication Configuration with subjectAlternativeName
authentication -->

```

```

<!-- (without HP SSO support) -->
<security:http pattern="/idm/v0/login" use-expressions="true" auto-config="false">
  <security:http-basic />
    <security:custom-filter ref="requestTokenCompositeFilter" position="FIRST"/>

    <security:custom-filter position="LAST" ref="cacFilter" />
    <security:custom-filter position="X509_FILTER"
ref="cacX509AuthenticationFilter" />
  </security:http>

  <bean id="cacFilter"
class="com.hp.ccue.identity.filter.certificate.CertificateFilter">
    <property name="generateTokenUtil" ref="generateTokenUtil" />
    <property name="tokenFactory" ref="tokenFactory"/>
    <property name="loginRedirectionHandler" ref="loginRedirectionHandler"/>
    <property name="authenticationProvider" ref="cacLdapAuthProvider"/>
  </bean>
  <!-- END Certificate Authentication Configuration with subjectAlternativeName
authentication -->

```

- c. Locate the line “<!-- START Certificate Authentication (beans) -->” and uncomment the content below the same so that it appears as follows.

```

<!-- START Certificate Authentication (beans) -->
<bean id="cacX509AuthenticationFilter"
class="org.springframework.security.web.authentication.preauth.x509.X509AuthenticationFilter">
    <property name="authenticationManager" ref="authManager" />
    <property name="principalExtractor" ref="customX509Extractor" />
</bean>

    <bean id="customX509AttrPreAuthAuthProvider"
class="org.springframework.security.web.authentication.preauth.PreAuthenticatedAuthenticationProvider">
    <property name="preAuthenticatedUserDetailsService"
ref="customAuthenticationUserDetailsService" />
  </bean>

    <bean id="customAuthenticationUserDetailsService"
class="org.springframework.security.core.userdetails.UserDetailsServiceByServiceWrapper">
    <property name="userDetailsService" ref="cacUserDetailsService" />
  </bean>

    <bean id="customX509Extractor"
class="com.hp.ccue.identity.filter.certificate.CustomX509PrincipalExtractor">
    <property name="x509Attribute" value="{idm.cac.x509Attribute:subjectDN}" />

```

```

        <property name="regex" value="\${idm.cac.regex:CN=(.*?),}" />
        <property name="sanType" value="\${idm.cac.san.type:OtherName}" />
        <property name="UPNResolver" ref="userPrincipalNameResolver" />
    </bean>

    <bean id="userPrincipalNameResolver"
class="com.hp.ccue.identity.filter.certificate.CsaBouncyCastleUpnExtractor" />

    <!-- END Certificate Authentication (beans) -->

```

- d. Locate the following line “<!--Pre authentication provider for CAC with subjectAlternativeName authentication -->” and uncomment the line below the same so that it appears as follows.

```

<!--Pre authentication provider for CAC with subjectAlternativeName
authentication -->
<security:authentication-provider ref="customX509AttrPreAuthAuthProvider" />

```

6. Save the file and exit.

## Configure Marketplace Portal for CAC authentication based on SAN when HP SSO is enabled

1. Navigate to the `$CSA_HOME/jboss-as/standalone/deployments/idm-service.war/WEB-INF/spring` directory.
2. Make a backup copy of the `applicationContext-security.xml` file.
3. Open the `applicationContext-security.xml` file in a text editor and do the following:

- a. Locate the following comments:

```

<!-- START Certificate Authentication Configuration -->
<!-- START with HP SSO support -->

```

- b. Comment the following content after these comments so that it appears as follows. Please ignore if it's already commented.

```

<!--
    <security:http pattern="/idm/v0/login" use-expressions="true" auto-
config="false">
        <security:http-basic />
        <security:custom-filter ref="hpssoProvidedFilter" before="PRE_AUTH_FILTER"
/>
        <security:custom-filter ref="hpssoIntegrationFilter"
after="PRE_AUTH_FILTER" />
        <security:custom-filter ref="requestTokenCompositeFilter"
position="FIRST"/>
        <security:x509 subject-principal-regex="CN=(.*?)," user-service-
ref="cacUserDetailsService" />

```

```

        <security:custom-filter position="LAST" ref="cacFilter" />
</security:http>

<bean id="cacFilter"
class="com.hp.ccue.identity.filter.certificate.CertificateFilter">
    <property name="generateTokenUtil" ref="generateTokenUtil" />
    <property name="tokenFactory" ref="tokenFactory"/>
    <property name="tokenWriter" ref="hpssoTokenWriter" />
    <property name="loginRedirectionHandler" ref="loginRedirectionHandler"/>
        <property name="authenticationProvider" ref="cacLdapAuthProvider"/>
        <property name="auditAppender" ref="auditAppender"/>
</bean>
-->
c. Locate the lines "<START Certificate Authentication Configuration with subjectAlternativeName
authentication (with HP SSO support)" and uncomment the contents below the same so that it
appears as follows.

    <!-- START Certificate Authentication Configuration with
subjectAlternativeName authentication -->
    <!-- (with HP SSO support -->
    <security:http pattern="/idm/v0/login" use-expressions="true" auto-
config="false">
        <security:http-basic />
        <security:custom-filter ref="hpssoProvidedFilter" before="PRE_AUTH_FILTER"
/>
        <security:custom-filter ref="hpssoIntegrationFilter"
after="PRE_AUTH_FILTER" />
        <security:custom-filter ref="requestTokenCompositeFilter"
position="FIRST"/>
        <security:custom-filter position="LAST" ref="cacFilter" />
        <security:custom-filter position="X509_FILTER"
ref="cacX509AuthenticationFilter" />
    </security:http>

    <bean id="cacFilter"
class="com.hp.ccue.identity.filter.certificate.CertificateFilter">
    <property name="generateTokenUtil" ref="generateTokenUtil" />
    <property name="tokenFactory" ref="tokenFactory"/>
    <property name="tokenWriter" ref="hpssoTokenWriter" />
    <property name="loginRedirectionHandler" ref="loginRedirectionHandler"/>
        <property name="authenticationProvider" ref="cacLdapAuthProvider"/>
        <property name="auditAppender" ref="auditAppender"/>
</bean>

    <!-- END Certificate Authentication Configuration with subjectAlternativeName
authentication -->

```

- d. Locate the line “<!-- START Certificate Authentication (beans) -->” and uncomment the content below the same so that it appears as follows.

```
<!-- START Certificate Authentication (beans) -->
<bean id="cacX509AuthenticationFilter"
class="org.springframework.security.web.authentication.preauth.x509.X509Authenticati
tionFilter">
    <property name="authenticationManager" ref="authManager" />
    <property name="principalExtractor" ref="customX509Extractor" />
</bean>

<bean id="customX509AttrPreAuthAuthProvider"
class="org.springframework.security.web.authentication.preauth.PreAuthenticatedAut
henticationProvider">
    <property name="preAuthenticatedUserDetailsService"
ref="customAuthenticationUserDetailsService" />
</bean>

<bean id="customAuthenticationUserDetailsService"
class="org.springframework.security.core.userdetails.UserDetailsServiceWrapp
er">
    <property name="userService" ref="cacUserService" />
</bean>

<bean id="customX509Extractor"
class="com.hp.ccue.identity.filter.certificate.CustomX509PrincipalExtractor">
    <property name="x509Attribute"
value="\${idm.cac.x509Attribute:subjectDN}" />
    <property name="regex" value="\${idm.cac.regex:CN=(.*?),}" />
    <property name="sanType" value="\${idm.cac.san.type:OtherName}" />

    <property name="UPNResolver" ref="userPrincipalNameResolver" />
</bean>

<bean id="userPrincipalNameResolver"
class="com.hp.ccue.identity.filter.certificate.CsaBouncyCastleUpnExtractor" />

<!-- END Certificate Authentication (beans) -->
```

- e. Locate the following line “<!--Pre authentication provider for CAC with subjectAlternativeName authentication -->” and uncomment the line below the same so that it appears as follows.

```
<!-- Pre authentication provider for CAC with subjectAlternativeName
authentication-->
<security:authentication-provider ref="customX509AttrPreAuthAuthProvider" />
```

- f. Within the `<!-- START Certificate Authentication Configuration -->` section, locate the “START without HP SSO support” section. Verify that the following content after this comment is commented out. If they are not commented out, you should comment them out.

```
<!--
<security:http pattern="/idm/v0/login" use-expressions="true" auto-config="false">
    <security:http-basic />
        <security:custom-filter ref="requestTokenCompositeFilter"
position="FIRST"/>
            <security:x509 subject-principal-regex="CN=(.*?)," user-service-
ref="cacUserDetailsService" />
                <security:custom-filter position="LAST" ref="cacFilter" />
        </security:http>

    <bean id="cacFilter"
class="com.hp.ccue.identity.filter.certificate.CertificateFilter">
        <property name="generateTokenUtil" ref="generateTokenUtil" />
        <property name="tokenFactory" ref="tokenFactory"/>
        <property name="loginRedirectionHandler" ref="loginRedirectionHandler"/>
        <property name="authenticationProvider" ref="cacLdapAuthProvider"/>
    </bean>
-->
```

- g. Save the file and exit.

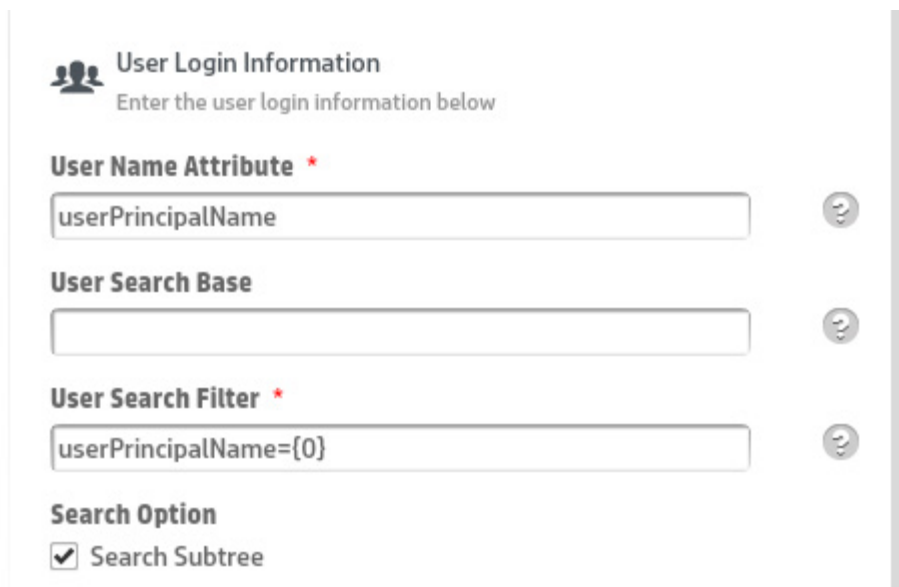
# Start HP CSA

Start the following services

1. HP Cloud Service Automation
2. HP Marketplace Portal
3. HP Search
4. Elasticsearch

## LDAP server configuration for CAC authentication based on UPN

Please set the “User Name Attribute” field and “User Search Filter” field to “**userPrincipalName**” and “**userPrincipalName={0}**” respectively in the LDAP server configuration for the Organization for CAC authentication based on UPN(UserPrincipalName) to be successful. Please refer to the below screenshot for reference.



The screenshot shows a configuration page titled "User Login Information" with the instruction "Enter the user login information below". It contains the following fields and options:

- User Name Attribute \***: A text input field containing "userPrincipalName".
- User Search Base**: An empty text input field.
- User Search Filter \***: A text input field containing "userPrincipalName={0}".
- Search Option**: A checkbox labeled "Search Subtree" which is checked.

Each text input field has a help icon (question mark) to its right.

**Note:** LDAP configuration will need to be similarly changed in OO and other products if HP SSO is enabled for CAC authentication based on UPN.

---

## Send documentation feedback

If you have comments about this document, you can send them to [clouddocs@hpe.com](mailto:clouddocs@hpe.com).

---

## Legal notices

### Warranty

The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without notice.

### Restricted rights legend

Confidential computer software. Valid license from Hewlett Packard Enterprise required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

### Copyright notice

© Copyright 2016 Hewlett Packard Enterprise Development LP

### Trademark notices

Adobe® is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

RED HAT READY™ Logo and RED HAT CERTIFIED PARTNER™ Logo are trademarks of Red Hat, Inc.

The OpenStack word mark and the Square O Design, together or apart, are trademarks or registered trademarks of OpenStack Foundation in the United States and other countries, and are used with the OpenStack Foundation's permission.

### Documentation updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.



- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to the following URL and sign-in or register: <https://softwaresupport.hp.com>.

Select Manuals from the Dashboard menu to view all available documentation. Use the search and filter functions to find documentation, whitepapers, and other information sources.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your Hewlett Packard Enterprise sales representative for details.

## Support

Visit the Hewlett Packard Enterprise Software Support Online web site at <https://softwaresupport.hp.com>.